Вопросы обеспечения энергетической безопасности инфраструктуры электронной науки

Тахмасиб Фаталиев[1], Шакир Мехтиев[2]
[1,2]Институт Информационных Технологий НАНА, Баку, Азербайджан
[1]depart3@iit.science.az, [2]depart11@iit.science.az

***Аннотация*– Статья посвящена вопросам обеспечения энергетической безопасности инфраструктуры э-науки. Рассмотрена инфраструктура э-науки, как составной части современной научно-исследовательской деятельности, и показано, что организация ее непрерывной и эффективной деятельности существенно зависит от решения проблем энергетической безопасности. Проанализированы концептуальные вопросы в этой области и предложена система, обеспечивающая энергетическую безопасность инфраструктуры э-науки.**

Ключевые слова– инфраструктура электронной науки, энергобезопасность, надежность, угрозы, центр обработки данных, AzScienceNet.

I. Введение

Бесперебойная работа энергетических систем является необходимым фактором функционирования и развития современного общества. Любые аварии в энергосистемах наносят ощутимые убытки различным отраслям промышленного производства, финансовым структурам, а также приводят к нарушению нормальной деятельности научного сектора и к отказам в работе его высокотехнологичного оборудования, создают угрозы жизни и безопасности людей. Проблемы с энергетической безопасностью (ЭБ) актуальны для различных стран вне зависимости от их экономического развития. Например, произошедшая в результате природных явлений авария в энергосистеме Нью-Йорка (New-York, USA, 1977 г.) вызвала сбои в работе городских служб, произошла остановка электротранспорта и т.п. [1]. Длительные простои, связанные с устранением возникших неисправностей, привели и к финансовым потерям. Аварии, произошедшие на Чернобыльской атомной электростанции (АЭС) (Украина) в 1986 г. и на Фукусимской АЭС (Япония) в 2011 г., расцениваются как крупнейшие по материальному и экономическому ущербу и степени опасного воздействия на окружающую среду и жизни людей. В [2] приведены примеры известных энергетических аварий, произошедших в мире за период 2003 -2015 гг.

Отметим, что современное общество характеризуется широким внедрением информационно-коммуникационных технологий (ИКТ), которые тесно интегрированы в различные сферы деятельности. Эффективное и надежное функционирование ИКТ в большей степени, чем другие отрасли, зависит от ЭБ. Аварии в энергетических системах, как следствие угроз ЭБ, могут привести к падению интернет-трафика, сбоям в передаче данных, прекращению работы центров обработки данных (ЦОД), а также к информационным потерям, что в целом может повлиять на работу различных структур.

В предлагаемой работе рассмотрены вопросы ЭБ инфраструктуры электронной науки (э-науки), которая включает в себя научную компьютерную сеть, ЦОД, сетевые, вычислительные и информационные ресурсы научно-исследовательских институтов и университетов. Следует отметить, что основными целями э-науки являются совместная эффективная деятельность в виртуальном пространстве научных организаций, коллективов и ученых, повышение эффективности научного управления и исследовательских работ, развитие всех областей науки на уровне современных мировых стандартов и интеграция в мировую научную среду [3].

II. Особенности Проблем Энергетической Безопасности

Международное Энергетическое Агентство определяет ЭБ, как бесперебойную доступность источников энергии [4]. Некоторые авторы дополняют определение ЭБ низкой уязвимостью жизненно важных энергетических систем. Также к ЭБ относят способность энергосистемы постоянно выполнять свои функции в условиях возможных неблагоприятных ситуаций (техноэкономических, геополитических, природных и т.д.) с минимально допустимыми нарушениями в работоспособности поддерживаемой системы. Таким образом, под ЭБ понимается устойчивость энергосистемы к событиям, инцидентам или непредвиденным (чрезвычайным) обстоятельствам, вызывающим ненормальные системные условия, то есть сбои или перебои в компонентах системы. Рассмотрим некоторые совокупные свойства ЭБ [5].

DOI: 10.25045/NCInfoSec.2018.22

Эксплуатационная безопасность – это свойство энергосистемы поддерживать или восстанавливать приемлемую работоспособность после устранения последствий инцидентов. Она охватывает динамические проблемы управления сетью в режиме реального времени.

Гибкость – это свойство энергосистемы справляться с краткосрочной/среднесрочной изменчивостью генерации (например, возобновляемой энергии) и спросом, чтобы система оставалась в равновесии.

Адекватность – это свойство энергосистемы постоянно обеспечивать общий спрос на электроэнергию при нормальных условиях эксплуатации. Она обычно включает в себя: компонент достаточности генерации/хранения, компонент сети передачи/приема, распределительную сеть и компоненты достаточности конечного пользователя.

Устойчивость – это среднесрочное свойство энергосистемы нейтрализовать последствия сбоев и восстанавливать определенный уровень производительности.

Надежность – это долгосрочное свойство энергосистемы справляться с ограничениями или воздействиями, возникающими вне инфраструктуры.

Исходя из данных предпосылок можно предложить концепцию ЭБ э-науки, которая состоит из эффективного и устойчивого распределения полученной энергии, уменьшения потерь, обеспечения непрерывной работы инфраструктуры э-науки и предотвращения как внешних, так и внутренних угроз. Этим достигается надежное, эффективное и безопасное функционирование э-науки.

Следует отметить, что на практике часто путают понятия надежности и безопасности. Надежность и безопасность – это системные свойства, возникающие в результате взаимодействия различных компонентов сложных систем: аппаратного, программного, организационного и человеческого.

Надежность – это свойство системы выполнять заданные функции, сохраняя свои эксплуатационные показатели в течение требуемого промежутка времени или требуемой наработки. Безопасность – это свойство, характеризирующее степень безаварийности и функциональной безопасности системы. Статистические данные в связи с промышленными авариями за последние несколько десятилетий позволяют сделать вывод о том, что организационные и человеческие факторы играют значительную роль в риске системных сбоев и аварий на протяжении всего жизненного цикла системы. В то же время существенно увеличилась надежность аппаратных компонентов, особенно в энергетических системах, где требуются высокие стандарты безопасности. Современные энергетические системы в соответствии с заданными требованиями и критериями надежности обеспечивают эффективную работу на протяжении длительного срока службы с минимальными рисками для безопасности персонала и окружающей среды. Для обеспечения этого необходимо контролировать развитие технологических процессов путем надлежащего планирования, проведения измерений и мониторинга. С этой целью осуществляется техническое обслуживание (ТО), которое должно обеспечивать соответствие характеристик надежности и доступности систем и компонентов в соответствии с долгосрочными и краткосрочными требованиями планируемых производственных и нормативных директив при минимальных ресурсных затратах. Цель эффективного планирования ТО – сведение к минимуму незапланированных простоев. Решения должны приниматься в отношении того, какое технологическое оборудование требует стабильного мониторинга для поддержания его работоспособности и своевременности ТО с целью сведения к минимуму угрозы ЭБ. Перечислим основные возможные проблемы в достижении ЭБ:

А. Внешние угрозы. Имеют естественный, случайный, злонамеренный и системный характер.

Б. Многофакторность. Угрозы материализуются из-за неблагоприятных событий, возникающих из-за экономических или геополитических факторов.

В. Временные рамки. Угрозы бывают краткосрочные, среднесрочные и долгосрочные.

Г. Многодисциплинарность. Оценка ЭБ с точек зрения политической, стратегической, нормативной, научно-технической дисциплин.

Д. Ответственность выбора. Действия по предотвращению, смягчению и реагированию на угрозы ЭБ возлагается на личности, принимающие решения.

Е. Многомодельность. Возможны динамические и статические модели действий.

Ж. Многогранность. Свойства ЭБ можно разделить на эксплуатационную безопасность, гибкость, адекватность, устойчивость и надежность.

Перечень приведенных проблем ЭБ показывает сложность и актуальность их решений в глобальном и локальном масштабах. В нашем случае следует ориентироваться на комплексный подход к решению этих проблем.

III. Энергетическая Безопасность Э-Науки

Э-наука, являясь сложной системой, объединяющая программные и технические средства, предоставляет многочисленные возможности в решении задач хостинга, хранилища данных, облачного сервиса, электронной почты, электронной библиотеки, роуминг-сервиса академической сети и т.п. Достижение этих задач требует максимально надежного и безопасного функционирования инфраструктуры э-науки, так как ошибки в их работе или

же временный простой оборачиваются потерями различного рода (иногда и невосполнимыми).

В решении научно-технических задач э-науки основные функции принадлежат ЦОД, структурно состоящего из информационной, телекоммуникационной и инженерной инфраструктур.

А. Информационная инфраструктура. Включает серверное оборудование и обеспечивает обработку и хранение информации.

Б. Телекоммуникационная инфраструктура. Обеспечивает взаимосвязь элементов ЦОД и передачу данных.

В. Инженерная инфраструктура. Обеспечивает поддержание заданных технических параметров для нормального функционирования основных систем ЦОД.

ЭБ является необходимым условием для всех операций ИКТ оборудования, то есть процессорных и запоминающих устройств, сетевых компонентов и линий передачи данных. Одновременно с ИКТ оборудованием, актуальным является надежность и безотказность в работе инженерной инфраструктуры, которая в общих случаях включает системы охлаждения, кондиционирования воздуха, пожарного надзора и пожаротушения, безопасности и контроля доступа, освещение. Высокая степень ЭБ и готовности технических средств требует обеспечения высокого качества электроэнергии и недопущение перерывов в электроснабжении. В идеале должен быть разработан надежный комплекс, состоящий из систем бесперебойного и гарантированного питания, резервных генераторов, стабилизаторов напряжения для обеспечения чистого электропитания компьютерной техники, систем освещения и внутреннего электроснабжения. С прикладной точки зрения, степень безопасности (отказоустойчивости) сложного электронного оборудования и, следовательно, стоимость услуг, отражаются в т. н. классе безопасности Tier стандарта TIA/EIA942 [6]. Для каждого из выделенных уровней надежности в этом документе приводится описание, требования и рекомендации к таким системам и элементам, как например архитектурные решения, ЭБ, охлаждение, безопасность, противопожарные системы, структурированные кабельные системы, системы кабелепроводов и телекоммуникации.

Согласно TIA/EIA942 первый (базовый) уровень надежности ЦОД – Tier 1. Ошибки и отказы в работе систем и оборудования на этом уровне приводят к сбоям в работе всего ЦОД и, следовательно, к отказам в функционировании э-науки. На этом уровне инженерная инфраструктура предназначена только для удовлетворения текущих потребностей, то есть для работы без резервирования и избыточных ресурсов. Коэффициент отказоустойчивости равняется 99,671 %.

Второй уровень надежности ЦОД – Tier 2, который предполагает небольшой уровень резервирования работоспособности системы и имеет небольшие избыточные ресурсы в инженерных системах. Коэффициент отказоустойчивости 99,749 %.

Третий уровень надежности ЦОД – Tier 3. Данный уровень надежности позволяет провести ремонтно-профилактические работы без остановки процессов в ЦОД. Коэффициент отказоустойчивости – 99,982 %.

Четвертый уровень надежности – Tier 4. Это отказоустойчивый ЦОД с резервированием и дублированием всех систем, позволяющий выполнять любые плановые и внеплановые работы без прерывания работы. Коэффициент отказоустойчивости 99,995 %.

Однако, это не единственный стандарт. Существует также стандарт BICSI 002 2010, который определяет пять классов готовности ЦОД на основе четырех критериев: резервирование компонентов; резервирование систем; использование продуктов с определенным уровнем качества и меры противодействия любым внешним воздействиям, включая природные явления [7].

Другой стандарт CENELEC EN 50600 определяет минимальные требования для инфраструктуры ЦОД всех форм и размеров. В этом стандарте установлены меры по защите от природных явлений, экологических событий и несанкционированного доступа.

Стандарт ISO/IEC 30134 устанавливает требования к возобновляемой энергии, коэффициенту энергоэффективности и ключевым показателям эффективности ЦОД.

Угрозы ЭБ, могущие оказать влияние на работу ЦОД, условно можно разделить на три группы. Первая группа представляет собой ординарные угрозы – вероятные отказы и аварии, которые являются предметом исследований надежности и ТО системы энергообеспечения. Для компенсации таких возмущений предусматриваются различные формы резервирования мощностей по производству и передачи энергии, структурных решений по обеспечению гарантированного энергообеспечения отдельных категорий потребителей, выбор стратегий ТО. Во вторую группу входят неординарные угрозы ЭБ из-за природных, техногенных, экономических, социально-политических и управленческих рисков. В третью группу входят угрозы, связанные с информационной безопасностью. В связи с возникновением, широким распространением и внедрением Интернета вещей и *Smart grid* данный тип угроз также может спровоцировать проблемы в ЭБ. Угрозами в данном случае могут стать кибератаки, направленные на объекты генерации, управления (SCADA), передачи и потребления энергоресурсов. Примером первой подобной кибератаки стала атака на украинские электростанции, в ходе которой злоумышленники с помощью фишинга и вредоносной программы *BlackEnergy* атаковали систему управления

телемеханикой, смогли прекратить подачу электроэнергии и препятствовали работам по восстановлению работоспособности системы [8].

Характеристиками угроз ЭБ, потенциально влияющими на безопасность работы ЦОД, могут быть следующие параметры:

- Объект воздействия.
- Продолжительность воздействия.
- Природа происхождения (естественная, случайная, злонамеренная и системная).

На основе вышеуказанных критериев надежности и свойств ЭБ была предложена модель схемы энергообеспечения ЦОД в среде AzScienceNet (рис.1).

Рис.1. Схема энергообеспечения с однократным резервированием

При инцидентах или прерываниях в центральной энергосети по сигналам от блока управления резервный дизель-генератор в течение нескольких секунд выходит на рабочий режим. Смарт-коммутатор в зависимости от входов энергоснабжения (внешняя электросеть или дизель-генератор) обеспечивает приоритетное функционирование основных систем ЦОД – серверного и телекоммуникационного оборудований. Источники бесперебойного питания обеспечивают непрерывное энергообеспечение в течение переходных процессов запуска и переключений автоматики.

Особая роль в обеспечении эффективного функционирования подобных систем возлагается на ТО. Современные ИКТ, интернет, в особенности, WEB 2.0 и Интернет вещей сделали доступной технологию электронного ТО (*e-maintenance*). С ее помощью осуществляется дистанционный мониторинг основных контрольных точек в энергообеспечении и автоматическое оповещение службы ТО [9]. Таким образом, предложенная модель обеспечивает устойчивость к угрозам ЭБ, т.е. способна реагировать на события и инциденты, вызывающие ненормальные системные условия или непредвиденные обстоятельства с минимально допустимыми нарушениями работоспособности.

IV. Заключение

Решение проблем ЭБ играет существенную роль в формировании надежной инфраструктуры э-науки, ее эксплуатации и развитии. Проведенный анализ в этой области показал, что ЭБ требует комплексного подхода. Надежность и ЭБ инфраструктуры э-науки является существенным фактором в обеспечении ее информационной безопасности. Предложенная модель энергообеспечения инфраструктуры э-науки с интеллектуальным ТО позволит достичь оптимальных решений в области ЭБ.

Литература

[1] J. Latson, “Why the 1977 blackout was one of New York’s darkest hours,” 13 july 2017. http://time.com/3949986/1977-blackout-new-york-history

[2] O.P. Veloza, and F. Santamaria, “Analysis of major blackouts from 2003 to 2015: Classification of incidents and review of main causes,” The Electricity Journal, 2016, Vol. 29, No. 7, pp. 42-49.

[3] T. Fətəliyev, “Elektron elmin təhlükəsizliyinin təmin edilməsi məsələləri haqqında,” İnformasiya cəmiyyəti problemləri, 2016, №1, ss. 56-62.

[4] A. Cherp and J. Jewell, (2014). “The concept of energy security. Beyond the four As,” Energy Policy, 2014, 75(c), pp. 415-421. DOI: 10.1016/j.enpol.2014.09.005

[5] F. Profumo, E. Bompard, and G. Fulli, “Electricity security: models and methodsfor supporting the policy decision making in the European Union,” 2016, Thesis for: Doctorate in Electrical Engineering.

[6] Data Center standards (TIERS I-IV). https:// www.colocationamerica.com/data-center/tier-standards-overview.htm

[7] А. Чернобровцев, “Как построить ЦОД: лучшие практики,” Computerworld Россия, 2010, № 32. https://www.osp.ru/ cw/2010/32/13004588/

[8] R. M. Lee, M. J. Assante, T. Conway, “Analysis of the cyber attack on the ukrainian power grid,” 2016, Electricity Information Sharing and Analysis Center (E-ISAC), 23 p.

[9] T. Fətəliyev, Ş. Mehdiyev, “Şəbəkə mühitində elektron texniki xidmətin təşkili məsələləri,” Proqram mühəndisliyinin aktual elmi-praktiki problemləri, 2016, ss. 291-293.

ENERGY SECURITY ISSUES IN E-SCIENCE INFRASTRUCTURE

Tahmasib Fataliyev[1] and Shakir Mehdiyev[2]

Institute of Information Technology of ANAS, Baku, Azerbaijan

[1]depart3@iit.science.az, [2]depart11@iit.science.az

Abstract -- The article is devoted to the issues of ensuring the energy security of the e-science infrastructure. The necessity of the infrastructure of e-science as an integral part of modern research activities is substantiated. It is shown that the continuous and effective activity of e-science depends on solving the problems of energy security. Conceptual issues in this area are analyzed and a system is proposed that ensures the energy security of the e-science infrastructure.

Keywords -- infrastructure of e-science, energy security, reliability, threats, data center, AzScienceNet